

E-DRP (DISASTER RECOVERY PLANNING) IN CIMA

A project submitted to Dean of Postgraduate Studies and Research in  
partial Fulfillment of the requirements for the degree  
Master of Science (Information Technology)  
University Utara Malaysia

By  
Rosanatrah binti Hj. Ramli

G.A.  
76.9  
D 348  
R 11.11  
R 11.11



**KOLEJ SASTERA DAN SAINS**  
(College of Arts and Sciences)  
Universiti Utara Malaysia

**PERAKUAN KERJA KERTAS PROJEK**  
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa  
(I, the undersigned, certifies that)

**ROSANATRAH BT HJ. RAMLI**  
**(804101)**

calon untuk Ijazah  
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk  
(has presented his/her project of the following title)

**E-DRPC (DISASTER RECOVERY PLAN) IN CIMA**


seperti yang tercatat di muka surat tajuk dan kulit kertas projek  
(as it appears on the title page and front cover of project)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan  
dan meliputi bidang ilmu dengan memuaskan.  
(that this project is in acceptable form and content, and that a satisfactory  
knowledge of the field is covered by the project).

Nama Penyelia  
(Name of Supervisor) : **DR. AZIZAH HJ. AHMAD**

Tandatangan  
(Signature) :  Tarikh (Date) : 21/10/10

Nama Penilai  
(Name of Evaluator) : **MR. MUHAMAD SHAHBANI ABU BAKAR**

Tandatangan  
(Signature) :  Tarikh (Date) : 21/10/10

**DEAN OF POSTGRADUATE STUDIES AND RESEARCH OFFICE  
UNIVERSITI UTARA MALAYSIA**

**PERMISSION TO USE**

In presenting this partial fulfillment of the requirements for a postgraduate degree from the Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this in any manner in whole or in part, for scholarly purposes may be granted by my supervisor(s) or in their absence by the Dean of the Postgraduate Studies and Research. It is understood that any copying or publication or use of this parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from me.

Requests for permission to copy or to make other use of materials in this, in whole or in part, should be addressed to

Dean of Postgraduate Studies and Research  
College of Arts and Sciences  
Universiti Utara Malaysia  
06010 UUM Sintok  
Kedah Darul Aman  
Malaysia

## **ABSTRAK**

Projek ini menerangkan dan memaparkan rancangan pemulihan bencana untuk organisasi perkilangan dan perindustrian. Cement Industries of Malaysia Berhad (CIMA) diambil sebagai kajian kes. Melalui rancangan pemulihan ini, beberapa langkah telah dipertingkatkan dan diperbaiki seperti penilaian risiko dan analisis terhadap perjalanan proses perniagaan ketika berlakunya bencana. Kajian ini menumpukan kepada beberapa jenis bencana iaitu kebakaran, kegagalan perkakasan dan perisian, kegagalan rangkaian (LAN & WAN), kerosakan pendingin hawa, kegagalan elektrik berfungsi, dan virus. Rancangan pemulihan adalah amat penting bagi organisasi perkilangan dan perindustrian untuk menyokong aplikasi perniagaan dan memastikan proses perniagaan berjalan seperti sediakala. Sekiranya bencana terjadi, ia akan mengganggu operasi perniagaan yang melibatkan penggunaan perkakasan dan perisian. Kajian ini juga turut menerangkan kaedah yang perlu diambil dalam fasa perancangan dan pelaksanaan pemulihan bencana. Cadangan kerangka kerja pemulihan ini merangkumi operasi sebelum bencana, ketika bencana dan proses atau prosedur yang perlu dilakukan selepas berlakunya bencana. Pelan pemulihan ini juga turut menerangkan operasi yang dilakukan untuk mengelakkan bencana seperti kegagalan perkakasan dan perisian. Akhir sekali, melalui aktiviti penyelidikan dan penilaian risiko dan analisis, telah memperkenalkan model Pemulihan Bencana. Model yang dibangun berdasarkan 3 teknik iaitu analisis data, formula dan pemerhatian. UML digunakan untuk mengilustrasi dan memvisualisasikan model keperluan. Prototaip sistem telah dibangunkan dengan aplikasi yang sesuai supaya kesan terhadap proses perniagaan dan aktiviti perkilangan dapat dilakukan dengan cara mudah dan difahami.

## **ABSTRACT**

This project presents a disaster recovery plan in manufacturing and industrial organizations. Cement Industries of Malaysia Berhad headquarter (CIMA HQ) is taken as a case study. The proposed strategies and recommendations of disaster recovery plan which has been enhanced and improved by researcher based on risk assessment and business impact analysis. The type of disaster in this study focuses on fire, hardware and software failure, network failure (LAN & WAN), breakdown of air conditioner, power failure) no electrical supply and virus and malicious attacks. Disaster Recovery Planning is becoming a necessity for manufacturing and industrial organizations to support critical business software applications during a major incident or disaster that can disrupt day-to-day operations that involve the utilization of the specified software applications and to ensure business processes continue as a normal. If disaster happens, it will disrupt business operations involving the use of hardware and software. This study also describes the methods that should be taken in the planning and execution phases of disaster recovery. The proposed framework includes the operations of recovery before disaster, during disaster and the process after disaster. This recovery plan also describes the operations that need to prevent disasters such as hardware and software failure. Finally, through the research and business impact analysis, has introduced a disaster recovery model. The developed model is based on three techniques of data analysis, formulation and observation. UML is used to illustrate and visualize the model needs. The system prototype was developed with the appropriate application to the impact on business processes and manufacturing activities had been done simple and understandable way.

## **ACKNOWLEDGEMENTS**

All praise is due to Allah, Most Gracious and Most Merciful. Without help and mercy, I would not have reached this far.

It would not be possible for me to complete the program and this study without the support of my supervisor. I would like to express my appreciation and thank to Dr. Azizah Bt. Hj. Ahmad for her support, guidance, correct the usage of language, and give a comment and idea. She is very patience in reading my proposal and drafts and gives a feedback as soon as possible. Her discussions and help are very much appreciated.

My sincere appreciation is for my family member for their support. To my father, Ramli Bin Samad, thank for his support and also to my mother, Chempawan Binti Said that always give an encouragement to me to complete the study and thanks to them because always pray for me. I also would like to thank to my beloved sister, Rosnajihah Binti Ramli for her guidance to develop the courseware.

I must convey my gratitude to my friends, Nur Wahidah Binti Rafiee, and Sa'amah Binti Hassan for their guidance, help and support. I hope this will give an inspiration to them to acquire knowledge through life-long learning journey in their lives.

'Syukor to Allah' for granting the time and knowledge to me for complete my program and this study.

## TABLE OF CONTENTS

PERMISSION TO USE.....	I
ABSTRAK (BAHASA MALAYSIA) .....	II
ABSTRACT (ENGLISH).....	III
ACKNOWLEDGMENTS .....	IV
LIST OF TABLE .....	IX
LIST OF FIGURES .....	X
LIST OF ABBREVIATIONS.....	XII
<b>CHAPTER ONE :INTRODUCTION .....</b>	<b>1</b>
1.1 Problem Statements .....	5
1.2 Research Objectives.....	6
1.3 Significance of the study.....	7
1.4 Scope and Limitations.....	8
1.5 Structure of the Report.....	8
1.6 Summary .....	10
<b>CHAPTER TWO : LITERATURE REVIEW.....</b>	<b>11</b>
2.1 CIMA Background.....	12
2.1.1 Objectives and Rules.....	15
2.1.2 Performance Measurements.....	16
2.1.3 Application Systems .....	17
2.1.4 System, Data and Network Security .....	19
2.1.5 Discover Recovery .....	20
2.2 What Is A Disaster ? .....	20
2.2.1 Threats and Impacts of Lack Business Continuity .....	21
2.3 Disaster Recovery Plan (DRP).....	22
2.3.1 The Needs for Disaster Recovery Planning .....	23
2.3.2 Matters of Concern by Developing DRP .....	24
2.4 Risk Assessment .....	24
2.4.1 Event and Fault Tree Analysis.....	29
2.5 Business Impact Analysis (BIA).....	30
2.6 Scada System .....	31

2.7 Requirement.....	33
2.8 Summary .....	34
<b>CHAPTER THREE : METHDOLOGY .....</b>	<b>35</b>
3.1 Methodology .....	35
3.1.1 Phase 1 - Planning and Limitation .....	38
3.1.2 Phase 2 - Risk Assessment and Business Impact Analysis .....	38
3.1.3 Phase 3 - Strategy Selection.....	39
3.1.4 Phase 4 - Plan Development .....	40
3.1.5 Phase 5 - Testing.....	40
<b>CHAPTER FOUR : SYSTEMS ANALYSIS AND DESIGN .....</b>	<b>42</b>
4.1 System Requirements.....	42
4.1.1 Functional Requirements .....	42
4.1.2 Non- Functional Requirements .....	43
4.2 Use Case Diagram and Specification.....	44
4.2.1 View Risk Evaluation .....	45
4.2.2 View Critical Application and System Availability .....	46
4.2.3 View Cement Stock Statistic .....	47
4.2.4 View Cement Financial Impact .....	48
4.3 Activity Diagram .....	49
4.3.1 View Risk Evaluation .....	49
4.3.2 View Critical Application and System Availability .....	50
4.3.3 View Cement Stock Statistic .....	51
4.3.4 View Cement Financial Impact .....	52
4.4 Sequence Diagram .....	53
4.4.1 View Risk Evaluation .....	53
4.4.2 View Critical Application and System Availability .....	54
4.4.3 View Cement Stock Statistic .....	55
4.4.4 View Cement Financial Impact .....	56
4.5 Collaboration Diagram.....	57
4.5.1 View Risk Evaluation .....	57
4.5.2 View Critical Application and System Availability .....	58
4.5.3 View Cement Stock Statistic .....	59
4.5.4 View Cement Financial Impact .....	60



4.6 Summary .....	61
<b>CHAPTER FIVE : RESULTS AND FINDINGS.....</b>	<b>62</b>
5.1 Risk Assessment .....	62
5.1.1 Level of Critically .....	63
5.1.2 Type of Disaster .....	64
5.1.3 Disaster or Threats .....	64
5.1.4 Identifying The Probability of Threat Occurring.....	65
5.2 Prioritizing Business Process .....	66
5.2.1 Procedures of Prioritizing Business Process.....	67
5.3 System and Recovery Strategies .....	71
5.3.1 Define System Recovery Requirement.....	72
5.3.2 Application Recovery Requirements .....	73
5.4 Network Recovery Strategies .....	73
5.4.1 Wide Area Network (WAN).....	74
5.4.2 Local Area Network (LAN).....	74
5.5 Resiliency Improvement Strategies .....	75
5.5.1 Disaster Preparedness Enhancement Strategies.....	75
5.5.2 Resiliency and Recovery Improvement .....	76
5.5.3 Control System Disaster Strategy .....	77
5.6 Business Impact Analysis .....	78
5.6.1 Risk Evaluation.....	81
5.6.2 Critical Application & System Availability.....	82
5.6.3 Intangible and Incalculable Impacts to CIMA.....	83
5.7 Problem Escalation and DR Activation .....	84
5.7.1 Escalation During Office Hour .....	84
5.7.2 Escalation After Office Hour .....	85
<b>CHAPTER SIX :DISSCUSSION OF THE RESULT .....</b>	<b>87</b>
6.1 Introductions .....	87
6.2 Discussion of the Objectives.....	88
6.3 Interface Design For The System Prototype .....	90
<b>CHAPTER SEVEN :RECOMMENDATIONS AND CONCLUSIONS .....</b>	<b>95</b>
7.1 Details Facilities Recommendations.....	96
7.1.1 Physical Security Perimeter Risk & Controls.....	96
7.1.2 Environmental Risk & Controls.....	97
7.1.3 Backup Recovery Risk & Controls.....	97

7.2 Disaster Recovery Procedures .....99

    7.2.1 Before Disaster.....99

    7.2.2 During Disaster .....100

    7.2.3 After Disaster .....101

7.3 Research Conclusion.....102

**REFERENCES.....104**

**APPENDICES .....107**

    APPENDIX I .....107

    APPENDIX II ..... 107

## **LIST OF TABLE**

Table 2.1	SWOT Analysis	17
Table 4.1	List of Functional Requirements	42
Table 4.2	List of Non-Functional Requirements	43
Table 5.1	Identification of Threats in the Business Process	64
Table 5.2	Identifying the Probability of Threat Occurring	66
Table 5.3	Impact to Business Process	66
Table 5.4	Prioritizing of Business Process	67
Table 5.5	Number of User	69
Table 5.6	Business Process Ranking	71
Table 5.7	System Recovery Requirements	72
Table 5.8	Applications to be protected and restored	73
Table 5.9	Applications Recovery Requirements	73
Table 5.10	Financial Impact	79
Table 5.11	Risk Evaluation	81
Table 5.12	Critical Application & System Availability	83

## **LIST OF FIGURES**

Figure 2.1	Recovery Time Objective Graph	31
Figure 2.2	SCADA System Concept	32
Figure 3.1	Research Design Methodology Adopted from (Vaishnavi & kuechler, 2004)	36
Figure 3.2	Business Continuity Process	37
Figure 3.3	System Development Life Cycle	37
Figure 3.4	Model of DRP Methodology	38
Figure 3.5	System Development Life Cycle Methodology	40
Figure 4.1	Use Case Diagram	44
Figure 4.2	View Risk Evaluation Use Case	45
Figure 4.3	View Critical Application & System Availability Use Case	46
Figure 4.4	View Cement Stock Statistics Use Case	47
Figure 4.5	View Financial Impact Statistic Use Case	48
Figure 4.6	View Risk Evaluation Activity Diagram	49
Figure 4.7	View Critical Application & System Availability Activity Diagram	50
Figure 4.8	View Cement Stock Statistics Activity Diagram	51
Figure 4.9	View Financial Impact Statistic Activity Diagram	52
Figure 4.10	View Risk Evaluation Sequence Diagram	53
Figure 4.11	View Critical Application & System Availability Sequence Diagram	54
Figure 4.12	View Cement Stock Statistics Sequence Diagram	55
Figure 4.13	View Financial Impact Statistic Sequence Diagram	56
Figure 4.14	View Risk Evaluation Collaboration Diagram	57
Figure 4.15	View Critical Application & System Availability Collaboration Diagram	58
Figure 4.16	View Cement Stock Statistics Collaboration Diagram	59
Figure 4.17	View Financial Impact Statistic Collaboration Diagram	60
Figure 5.1	Probability of Threat	65
Figure 5.2	Business Process Critically	68
Figure 5.3	Business Process Ranking	69
Figure 5.4	CIMA Group Overall Network Architecture	75
Figure 5.5	Medium Tolerable Downtime (MTD)	76
Figure 5.6	Recovery Strategy Diagram for Plant Control System	77
Figure 5.7	Risk Assessment Technique	82
Figure 5.8	During Office Hour Escalation Flow	84
Figure 5.9	After Office Hour Escalation Flow	85
Figure 6.1	Login Page	90

Figure 6.2	Main Page	90
Figure 6.3	Planning List to identify MTD and Stock of Cement Statistic	91
Figure 6.4	Cement Stock Statistic	91
Figure 6.5	Critical System and System Availability Report	92
Figure 6.6	Critical System and System Availability Planning	92
Figure 6.7	Creating new Risk Evaluation List	93
Figure 6.8	View Risk Evaluation Graph	93
Figure 6.9	Logout Page	94
Figure 7.1	Disaster Recovery Procedures – Before Disaster Happen	99
Figure 7.2	Disaster Recovery Procedures – During Disaster Happen	100
Figure 7.3	Disaster Recovery Procedures – After Disaster Happen	101

## **LIST OF ABBREVIATIONS**

CIMA	Cement Industries of Malaysia Berhad
ICT	Information and Communication Technology
ERP	Enterprise Resource Planning
CDRP	Computer Disaster Recovery Plan
RA	Risk Assessment
BIA	Business Impact Analysis
CDRP	Control Disaster Recovery Plan
ERP	Enterprise Resource Planning
PLC	Programmable Logic Control
SCADA	Supervisory Control and Data Acquisition
LAN	Local Area Network
WAN	Wide Area Network
MTD	Minimum Tolerable Downtime
RTO	Recovery Time Objective
RPO	Recovery Point Objective
WTC	World Trade Center
MyCERT	Malaysian Computer Emergency Response Team
NISER	National ICT Security and Emergency Response Team

# **CHAPTER ONE**

## **INTRODUCTION**

Information and Communication Technology (ICT) has become embedded in the framework of virtually every aspect of a business. Computing is no longer found doing only background processing. Instead, critical business data can be found across the enterprise on desktop, personnel computers and departmental local area networks, as well as in the data center. The same information technology driving new sources of competitive advantage also has created new expectations and vulnerabilities. Key business initiatives such as plant systems, enterprise resource planning (ERP), supply chain management, customer relationship management and e-business have made continuous, ubiquitous access to information crucial to an organization. ICT facilities have potential to deliver immediate satisfaction or dissatisfaction to organizations and the public either to improve efficiencies or to feel the impact of disruption. Serious business interruptions are now measured in minutes rather than hours. Because electronic transactions and communications take place so quickly, the amount of work and business lost in an hour far exceeds the toll of previous decades. Hence, it is critical to the ICT facilities to maintain with the highest possible levels of availability and operability for continued business operations in any event.

Disasters are unexpected or sudden events that adversely affect the ability of organization to provide critical business function and affect any information center to perform its function in a timely and efficient manner. Planning for a

The contents of  
the thesis is for  
internal user  
only



## REFERENCES

- Adshead., A. (2003, September). Only 60% of firms have disaster recovery plans. *Computer Weekly*, p.6.
- Arnell., A. (1990). *Handbook of effective disaster recovery planning*. New York: McGraw-Hill Publishing.
- Bates., R.J. (1992). *Disaster recovery planning; network, telecommunications, and data communications*. New York: McGraw-Hill, Inc.
- Belfast Institute and North West Institute of Further and Higher Education. (2002). *Guidance on developing and maintaining computer disaster recovery plans in further and higher education*. Retrieved 10 August 2010, from <http://www.rsc-ni.ac.uk/technical/Disrec.pdf>
- Cerullo., Michael J., Steve R. (1994). *Planning for disaster*. The CPA Journal. 64(6), 34-38.
- Chang., S.-J.DiCesare., F.Golbogen., G. (1991). *Failure propagation trees for diagnosis in manufacturing systems*, IEEE. 21(4), 76-776.
- Cobb, C. (2003). *Network security for dummies*. New York: Wiley Publishing.
- Comprehensive Consulting Solutions, Inc. (2001). *Define what types of disaster that need to be planned for*. Retrieved 10 September 2010, from [http://wwwcompsoln.com/DRP2\\_whitepaper.pdf](http://wwwcompsoln.com/DRP2_whitepaper.pdf)
- Disaster Recovery Journal. (2004). *Business continuity glossary*. Retrieved 11 September 2010, from <http://www.drj.com/glossary/DRJ-Glossary.pdf>
- Eklund, B. (2001, December). Multi-faceted “continuity” plans are replacing simple data-recovery services in the wake of September 11. *Business Unusual*, pp.20-25.
- Edward, B. (2000). Developing a successful network disaster recovery plan. *Information Management & Computer Security*, 2(3), 37-42.
- Fallara, P.(2004). *Disaster recovery planning*. Potentials, IEEE. 22(5), 1-10.
- Farrokh, M. (2002). Evaluation and selection of antivirus and content filtering software. *Information Management and Computer Security*, 10(1), 28-32.
- Ferrarini, E.M. (2001). *How to create a disaster recovery plan before trouble strikes*. Retrieved 28 September 2010, from <http://www.naspa.com/PDF/2001/1201%PDF/70112006.pdf>

George, S.M. Wei Zhou Chenji, H. Myounggyu Won Yong Oh Lee Pazarloglou, A. Stoleru, R. Barooah, P. (2010). *DistressNet: a wireless ad hoc and sensor network architecture for situation management in disaster response*. Communications Magazine, IEEE. 48(3), 128-136.

Hayes, P.E. Hammons, A. (2002). Picking up the pieces: Utilizing disaster recovery project management to improve readiness and response time. Industry Applications Magazine, IEEE. 28(6), 27-36.

Harris, M. (2009). Disaster recovery. Engineering & Technology. 4(7), 26-29.

Hawkins, H. (1997). *Are you in the dark about disaster preparedness*. Kentucky Banker Magazine, pp.18-21.

Hiatt, C.J. (2000). *A primer for disaster recovery planning in an IT environment*. Hershey: Idea Group Publishing.

Ibrahim M.S., Fakharu'l-razi A., & Aini M.S (2003a). A review on disaster and crisis. *Disaster Prevention and Management*, 12(1), 24-32.

Ibrahim M.S., Fakharu'l-razi A., & Sa'ari M. (2003b). Technological disaster's criteria and models. *Disaster Prevention and Management*, 12(4), 305-311.

Infotech Research Group. (2003). *Building a comprehensive disaster recovery plan*. Retrieved 10 September 2010, from [http://www.infotech.com/drp/full\\_sample.pdf](http://www.infotech.com/drp/full_sample.pdf)

Kundu, S.C. (2004). Impact of computers disasters on information management: a study. *Industrial Management & Data System*, 104 (2), 136-143.

Maiwald, E., & Sieglein, W. (2002). *Security planning & disaster recovery*. California: McGraw-Hill Osborne

Pfleeger., Charles., & Pfleeger., S. (2003). *Security in Computing*. New Jersey: Prentice Hall.

Schmidt., N.(2001). If disaster strikes, can your business rise from the ashes?. IT Professional. 3(1), 57-59.

Shao., B.B.M. (2005). Optimal redundancy allocation for information technology disaster recovery in the network economy. Dependable and Secure Computing, IEEE Transactions. 2(3), 262-267.

Savage., M. (2002). Business continuity planning. *Work Study*, 51 (5), 254-261

Swann., J. (2004, February). Be prepared: disaster recovery strategies. *Community Banker*, pp. 40-44.

Toigo., Jon. (1996). *Disaster Recovery Planning: For Computers and Communication Resources*, New Jersey: Prentice Hall.

Toigo., Jon. (2000). *Disaster Recovery Planning: Strategy For Protecting Critical Information Assets*. New Jersey: Prentice Hall.

Toigo., Jon. (2003). *Disaster Recovery Planning: Preparing For The Unthinkable*, New Jersey: Prentice Hall.

T.Paulos. (2001). System Safety. Retrieved 21 August 2010, from <http://www.fault-tree.net/papers/paulos-pra-tutorial.pdf>

Voigt, S.Kemper, T.Riedlinger, T.Kiefl, R.Scholte, K.Mehl, H.(2007). Satellite Image Analysis for Disaster and Crisis-Management Support. *Geoscience and Remote Sensing, IEEE Transactions*. 45(6), 1520-1528.

Weaver., J. (2003). *Disaster response and recovery*. Retrieved 23 August 2010, from <http://www.hill.com/archive/pub/papers/2003/09/paper.pdf>

Wing., S.C. (2000). Success factors for IS disaster recovery planning in Hong Kong. *Information Management & Computer Security*, 8 (2), 80-86.